Security Analysis of Common Wireless Networking Implementations

Brian Cavanagh
CMPT 585
12/12/2005

The use of wireless networking to connect to the internet has grown by leaps and bounds in recent years. From the comfort of their own homes, or from the convenient setting of their local Starbucks, computer users are wirelessly connecting to the internet in staggering numbers. Of course, security implications abound when a wireless network is in use.

This paper will analyze the current state of security surrounding wireless networks. Particular attention will be paid to the implementations of Wireless Access Points (WAPs). As we will see, although a WAP may come with the means to enable stringent wireless security, they are very rarely properly configured, and encryption is very often not even enabled.

The most common means for securing a wireless network is WEP (Wired Equivalent Protocol) Encryption. This paper will examine WEP Encryption, showing different methods currently utilized to break this encryption.

The role of the hardware manufacturer will also be discussed. By looking at the factory default settings on three common WAPs, we will gain insight into the level of care taken by hardware manufacturers to help ensure the privacy of their consumers.

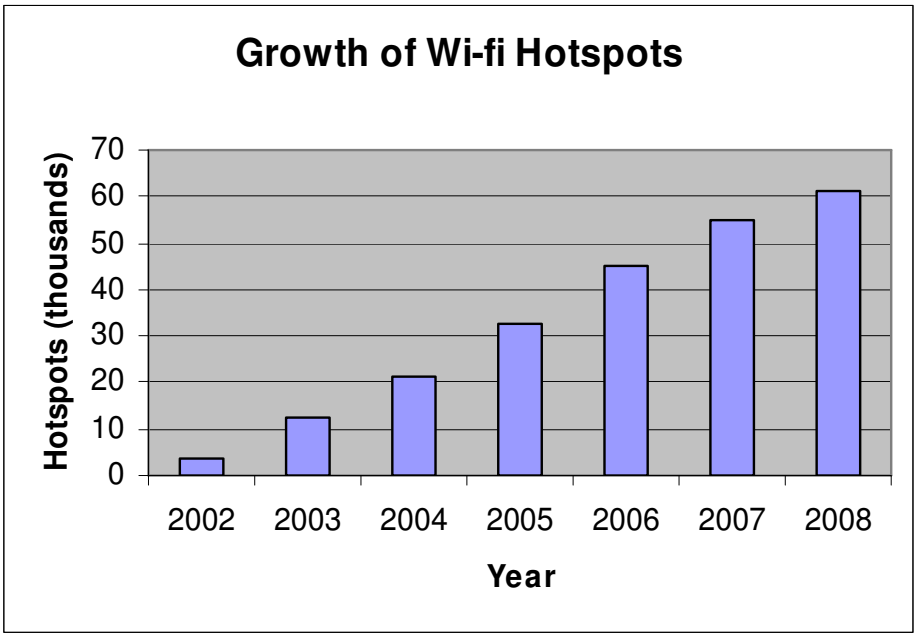
Growth of Wireless Networking

Since its inception, wireless networking has seen staggering year over year growth. As the use of broadband internet access continues to rise, more consumers will purchase network routers to allow the sharing of broadband access throughout the household. As with all computer hardware, the cost of network routers continues to plummet. Additionally, many routers now come bundled with wireless access point capabilities.

A user must simply purchase a cheap wireless network card in order to be able to access the internet from anywhere in their house. Wireless network cards for desktops computers (PCI) or notebook computers (PCMCIA) can now routinely be found for less than $25.

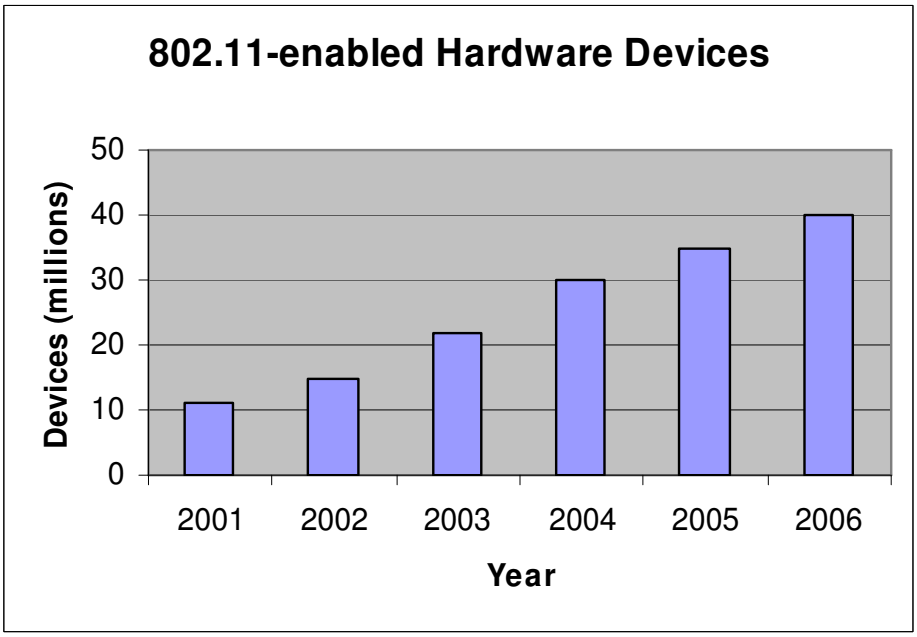
The adoption of broadband internet access combined with a decline in price for the requisite hardware has led to steady growth. The two figures below depict two examples of this.

Figure 1



Source: Telecommunications Industry Association

Figure 2



Source: In-Stat/MDR

As shown in Figure 1, it is projected that there will be 45,000 wireless hotspots available in 2006. This is up from less than 5,000 in 2002. A wireless hotspot is a wireless network that has been set up for public use. The type of service is now offered at many hotels, McDonald's and Starbucks (to name a few).

Figure 2 depicts the growth in sales of wireless hardware, with an estimated 40 million wireless-enabled hardware devices estimated to be sold in 2006. This includes both wireless routers and wireless network cards. Obviously, as these numbers continue to rise, so will the number of more savvy computer users looking to take advantage of those that are wireless-enabled but not mindful of their wireless security.

Typical Wireless Security Pitfalls

As will be shown later in this paper, the common wireless network user does very little, if anything, to secure their wireless network from the outside world. While there is no way to guarantee that any wireless network won't be compromised, there are some very easy ways to at least make a wireless network less attractive to the casual hacker. Three typical pitfalls are discussed below:

- **Default service set identifier (SSID)** – WAPs come set up with an SSID. This SSID is broadcast from the router to alert in-range users to its presence. There are two things that can be done to help make a network more secure.
    1. Change the default SSID – Hardware manufacturers generally use the same SSID for all of their equipment. They also use the same default password. If a user doesn't change the SSID and the corresponding password, a hacker can access the administration settings of the access point.
    2. Turn off the SSID broadcast – Many access points come equipped with the ability to not broadcast the SSID altogether. Although there are ways for a hacker to detect the network, turning off the SSID broadcast will help to make a network less appealing.

- **WEP Encryption** – WEP Encryption is a security protocol developed for use with WAPs. Although not very strong (as will be seen below), having encryption turned on makes it much more difficult to break into a network.

- **MAC Address Filtering** – Every piece of 802.11 hardware that is produced comes with its own MAC (Media Access Control) address. A WAP can be configured to only allow access to certain MAC addresses. This way, the owner of the network can configure the WAP to only allow traffic from devices that he or she owns. Again, this method of security is not insurmountable to an accomplished hacker, but will help keep out the average over-curious neighbor.

WEP Encryption

WEP Encryption is the most common wireless encryption method in use today. The overwhelming majority of WAPs available today come with WEP encryption available. WEP Encryption is based on the use of a symmetric key. Once WEP is enabled, all network devices wishing to gain access to the network must be able to supply the appropriate key.

WEP keys are either 64-bit or 128-bit. However, for both the 64-bit and 128-bit key, 24 bits are reserved for what is calling the Initialization Vector (IV). (This will be important later as the cracking of WEP is discussed). Rather than requiring a user to actually type 40 or 104 bits (depending upon the key size), most WAPs ask the user for a pass-phrase. The WAP then uses an algorithm to transform the pass-phrase into a key. Based on the design of the algorithm, this could open the door to the possibility of a dictionary attack, as many users will chose an English word as the pass-phrase used to generate their key. (Again, this will be significant the cracking of WEP is discussed).

Cracking WEP

This paper will discuss two popular methods employed to crack WEP – The FMS Attack and a dictionary attack. Although, there are a number of other methods available to crack WEP, the scope of this discussion is limited to these two.

The FMS Attack

The FMS Attack is the most common method for cracking WEP. It was conceived by Scott Fluhrer, Itsik Mantin, and Adi Shamir in their paper "Weakness in the key scheduling algorithm of RC4". The basis for the FMS attack is that the WEP key generation can result in what are called "weak IVs". As mentioned above, the IV is the first 24 bits of the key. The IV is also sent "in the clear" so it is available to anyone within range of the wireless network. Once a significant number of weak IVs have been captured by a potential hacker, they can be used to "back in" to the WEP key. Certain bits within the IV are essentially used to deduce the remaining bits in the key.

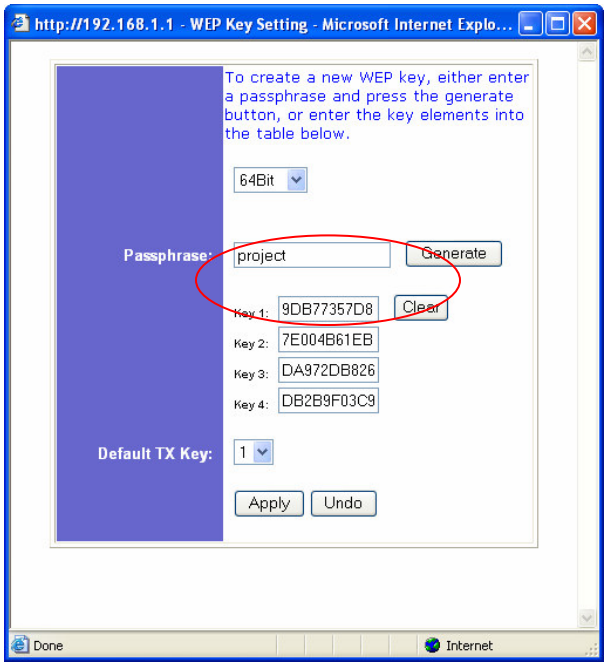
In order to study this attack, I set out to attack my own home wireless network. Many tools have been developed that employ the FMS attack; for this test I used a Linux-based tool called Airsnort. The hardware employed for this test is shown below:

- WAP – Linksys BEFW11S4v.2
- D-Link 520+ PCI Card
- Compaq W110 PCMCIA Card

The design of the attack was to "sniff" enough data on my wireless network so as to collect enough weak IVs to allow Airsnort to discover my key. In the interest of time, I

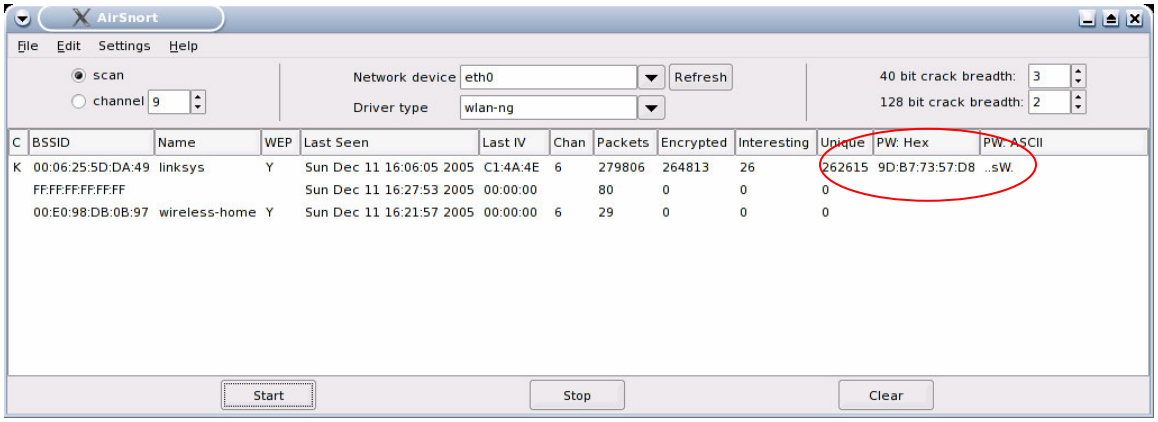
set my key to 64-bits as is shown in Figure 3 below. The pass-phrase I used was "project".

Figure 3



In order to collect enough packets to allow Airsnort to work, I began transferring a large (4GB) file wirelessly between 2 desktop computers on my network. Once this transfer began, Airsnort started collecting packets and analyzing the IVs. As can be seen from Figure 4 below, the key for my network was cracked in 2 hours and 15 minutes. Note: Airsnort labels weak IVs as "Interesting"

Figure 4


AirSnort
File Edit Settings Help
scan
channel 9
Network device eth0
Refresh
Driver type wlan-ng
40 bit crack breadth: 3
128 bit crack breadth: 2
C BSSID Name WEP Last Seen Last IV Chan Packets Encrypted Interesting Unique PW: Hex PW: ASCII
K 00:06:25:5D:DA:49 linksys Y Sun Dec 11 16:06:05 2005 C1:4A:4E 6 279806 264813 26 262615 9D:B7:73:57:D8 ..sW.
FF:FF:FF:FF:FF:FF Sun Dec 11 16:27:53 2005 00:00:00 80 0 0 0
00:E0:98:DB:0B:97 wireless-home Y Sun Dec 11 16:21:57 2005 00:00:00 6 29 0 0 0
Start
Stop
Clear

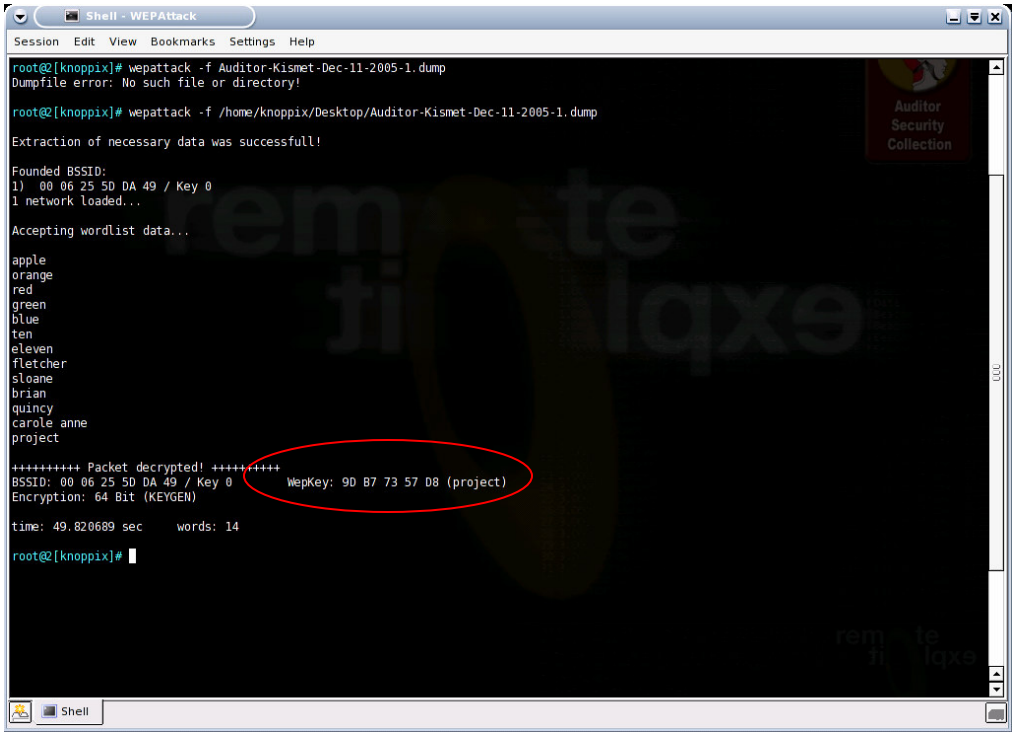
Obviously, in a real-world example, the hacker would not be able to initiate a file transfer in order to speed up the cracking process. There are, however, a variety of tools available that will ping the WAP with dummy data and force a response. Through these responses enough data can be obtained to ultimately crack WEP. Additionally, based on the locations of the network, a potential hacker could just wait until enough data was transmitted.

Dictionary Attack

As mentioned above, many WAPs use an algorithm in order to create the key. The user is first asked to enter a pass-phrase which is then used to generate the key. Obviously, with the genesis of the key being a user-entered string, this particular implementation of WEP is susceptible to a dictionary attack. A dictionary attack is the process of going through a file of words and testing each one to see if it matches the key.

I used a Linux-based tool called Wepattack to test this vulnerability. The exact same hardware set up was used as in the FMS attack above. Before a dictionary attack can be run, a small amount of network traffic must be collected into a dump file. To create the dump file, I used another Linux-based tool called Gkismet. Once enough data had been collected with Gkismet, I used Wepattack to attempt to break the WEP encryption. Figure 5 below shows that WEP was broken once I typed in the correct pass-phrase on the command line.

Figure 5



Obviously, entering possible pass-phrases one at a time is not a viable solution for using this tool. However, when using a freely-available word list of English words, the WEP encryption was once again easily cracked. (Note: In order to ensure the test would finish quickly, I changed my pass-phrase to "aardvark", as the word lists are in alphabetical order).

Default Settings of Wireless Access Points

We have learned that cracking WEP is a relatively easy process under the right conditions. However, from a hacker's point of view, it's quite a bit easier to break into a network with no security at all than into a network with WEP enabled. In that vein, I decided to look at WAPs currently offered by 3 of the large manufacturers of wireless networking equipment – Linksys, Netgear, and D-Link. In order to execute this study, I downloaded the user manual for the WAP from the manufacturer's website. In particular, I looked at the 3 WAPs below:

- Linksys WRT54G
- Netgear WPN824
- D-Link DI-634M

In every case, the default setting was no wireless encryption. Why would this be? Doesn't the manufacturer care about the privacy of its consumers? The answer, in short, is that they care more about their bottom line. Enabling WEP by default on the router would require the end user to enable it on each of their network devices. Although relatively easy, this would invariably lead to more support calls for the manufacturer, with each call costing them money. Therefore, the consumer is left to make sure they've turned on some sort of encryption for their network.

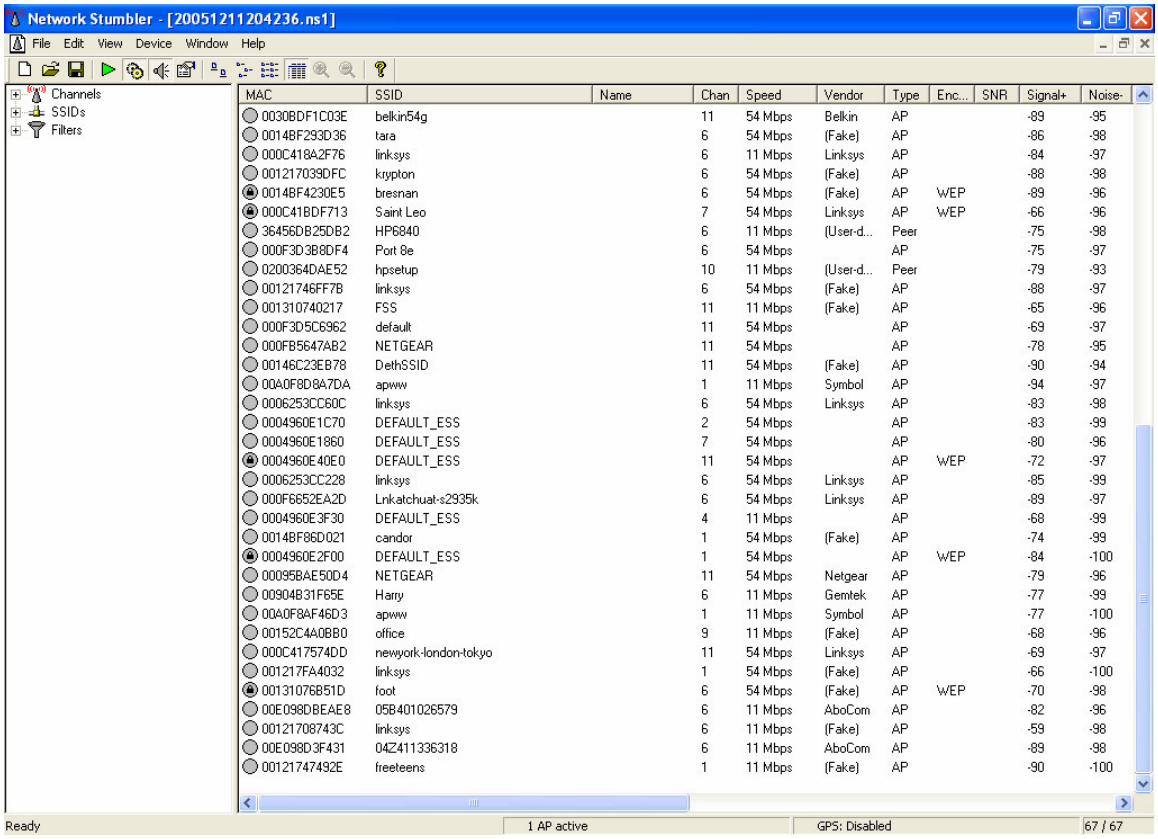
Wardriving

Wardriving is the activity of seeking out unprotected networks in order to find those networks with minimal security. Presumably the "wardriver" would either use the network for free internet access, or more deviously – to break into the network for personal gain.

Knowing that WAPs often have no security by default, I spent an evening driving around my town (Fair Lawn, NJ) to gather data on my neighbor's security practices. To do this I used a Windows-based tool called NetStumbler, which is able to detect wireless networks and report a good amount of details on them (MAC, SSID, Channel, Vendor, etc…).

My results can be seen in Figure 6 below:

Figure 6

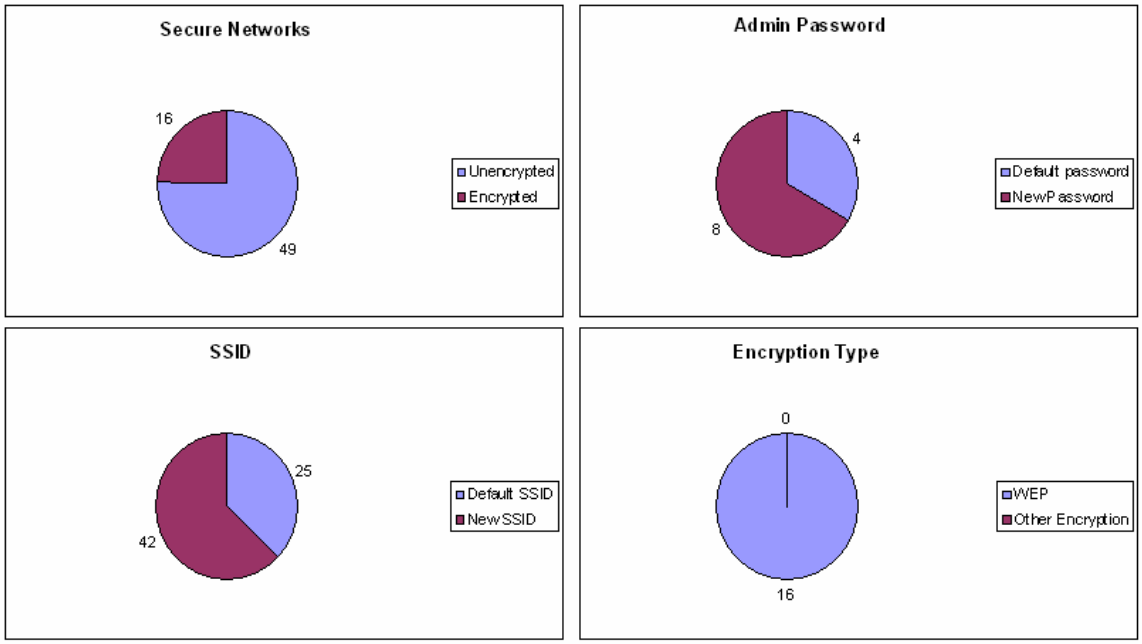

Network Stumbler - [20051211204236.ns1]
File Edit View Device Window Help
Channels
SSIDs
Filters
MAC SSID Name Chan Speed Vendor Type Enc... SNR Signal+ Noise-
0030BDF1C03E belkin54g 11 54 Mbps Belkin AP -89 -95
0014BF293D36 tara 6 54 Mbps (Fake) AP -86 -98
000C418A2F76 linksys 6 11 Mbps Linksys AP -84 -97
001217039DFC krypton 6 54 Mbps (Fake) AP -88 -98
0014BF4230E5 bresnan 6 54 Mbps (Fake) AP WEP -89 -96
000C41BDF713 Saint Leo 7 54 Mbps Linksys AP WEP -66 -96
36456DB25DB2 HP6840 6 11 Mbps (User-d... Peer -75 -98
000F3D3B8DF4 Port 8e 6 54 Mbps AP -75 -97
0200364DAE52 hpsetup 10 11 Mbps (User-d... Peer -79 -93
00121746FF7B linksys 6 54 Mbps (Fake) AP -88 -97
001310740217 FSS 11 11 Mbps (Fake) AP -65 -96
000F3D5C6962 default 11 54 Mbps AP -69 -97
000FB5647AB2 NETGEAR 11 54 Mbps AP -78 -95
00146C23EB78 DethSSID 11 54 Mbps (Fake) AP -90 -94
00A0F8D8A7DA apww 1 11 Mbps Symbol AP -94 -97
0006253CC60C linksys 6 54 Mbps Linksys AP -83 -98
0004960E1C70 DEFAULT_ESS 2 54 Mbps AP -83 -99
0004960E1860 DEFAULT_ESS 7 54 Mbps AP -80 -96
0004960E40E0 DEFAULT_ESS 11 54 Mbps AP WEP -72 -97
0006253CC228 linksys 6 54 Mbps Linksys AP -85 -99
000F6652EA2D Lnkatchuat-s2935k 6 54 Mbps Linksys AP -89 -97
0004960E3F30 DEFAULT_ESS 4 11 Mbps AP -68 -99
0014BF86D021 candor 1 54 Mbps (Fake) AP -74 -99
0004960E2F00 DEFAULT_ESS 1 54 Mbps AP WEP -84 -100
00095BAE50D4 NETGEAR 11 54 Mbps Netgear AP -79 -96
00904B31F65E Harry 6 11 Mbps Gemtek AP -77 -99
00A0F8AF46D3 apww 1 11 Mbps Symbol AP -77 -100
00152C4A0BB0 office 9 11 Mbps (Fake) AP -68 -96
000C417574DD newyork-london-tokyo 11 54 Mbps Linksys AP -69 -97
001217FA4032 linksys 1 54 Mbps (Fake) AP -66 -100
00131076B51D foot 6 54 Mbps (Fake) AP WEP -70 -98
00E098DBEAE8 05B401026579 6 11 Mbps AboCom AP -82 -96
00121708743C linksys 6 11 Mbps (Fake) AP -59 -98
00E098D3F431 04Z411336318 6 11 Mbps AboCom AP -89 -98
00121747492E freeteens 1 11 Mbps (Fake) AP -90 -100
Ready
1 AP active
GPS: Disabled
67 / 67

Those networks with some sort of encryption are denoted by the icon with a lock. It is immediately apparent that very few networks have any encryption at all. Of the 65 networks found, only 16 (25%) used encryption. Interestingly, 42 networks (65%) had changed the default SSID, which raises the question – If the user is savvy enough to change the default SSID, why not enable WEP? It is possible that some networks are left intentionally open to allow sharing of a broadband connection between neighbors.

Additionally, of the 12 users with the default SSID of "linksys", 4 had not changed the password for their router configuration page, thereby allowing anyone in range to change their router settings. Finally, of the 16 users that did enable encryption, every single one used WEP. A stronger encryption method called WPA (Wi-fi Protected Access) is now available but was not seen in used at all. Note: WPA is outside the scope of this paper as it focuses on actual implementations of wireless security. As proved by this exercise, WPA is not nearly as prevalent as WEP.

The results of the wardriving study are seen in Figures 7 – 10 below:

Figures 7 -10:



Conclusions

We have seen that there are a great many flaws inherent in wireless security today. However, this is not to say that a wireless network cannot be secure enough to give a user piece of mind. Specifically, although it is not by any means unbreakable, just by enabling WEP, users will likely make themselves less likely to be attacked. Also, by following some simple guidelines – changing the SSID, MAC address filtering, etc…, a user can make their less-savvy neighbor a much more appealing target to would-be hacker.

Those users that have highly sensitive data would be encouraged to employ other means of security. That is – using WPA instead of WEP, using a Virtual Private Network (VPN), or investing in a wireless Intrusion Detection System (IDS). However, for those just looking to share their broadband internet access at home, simply being mindful of enabling the tools already available should be enough to allow for piece of mind.

Works Cited

1. Vladimirov, Andrew; Gavrilenko, Konstantin; Mikhailovsly, Andrei. *Wi-Foo, The Secrets of Wireless Hacking.* Addison Wesley. 2004.

2. Fluhrer, Scott; Mantin, Itsik; Shamir, Adi. *Weakness in the key scheduling algorithm of RC4*. 2001.

3. Article on the proliferation of wireless networks: http://www.cnn.com/2005/TECH/ptech/12/12/wireless.city.ap/index.html

4. Overview of WEP Encryption: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy